CRAMM을 이용한 정보시스템 위험분석 및 관리
(장은신용카드의 사례연구)

김 법 진 · 한 인 구
(대 웅 그 룹) (한국과학기술원)

The Risk Analysis and Management for Information System using CRAMM:

Case of Korea Long Term Credit Card Corp.

Bob-jin Kim, Ingoo Han

Abstracts

In today's complex business world, managers should recognize a fundamental premise: it is not possible to have a risk-free data processing environment. Risk, therefore, must be managed. Being customers' security concern increased recently, the thesis studied risk analysis and management for information system by selecting a company having the highest sensitivity for customer's security. Consequently, the manager should decide to the countermeasure considering type, cost, state, and security level, etc. This thesis develops DSS (Decision Support System) for analyzing and selecting countermeasures, to assist manager's decision making.

1 Introduction

The risk analysis and management is a comprehensive concept for defining and analyzing the threat and vulnerability to organizational assets (data, software and hardware), and for assisting management in optimizing the return on investment of security services.

In today's complex business world, managers should recognize a fundamental premise: it is not possible to have a risk-free data processing environment. Risk, therefore, must be managed. The major questions facing management, when attempting to manage risks, are: What is the impact on business objectives and goals if the risks materialize? What security safeguards are available to reduce the unacceptable risks to an acceptable level? What security safeguards will provide the best return on investment?, etc.

Risk analysis and management, as currently practiced in the information system environments, can be viewed as a fairly specialized application of a problem-solving process generally referred to as the system approach. The essence of the system approach is that one should view an information system as a whole unit, rather than a group of separate parts.

Being customer's security concern increased recently, the researcher considers that one would rather mean analysis of a field than do full analysis of information system. Therefore, the thesis studied risk analysis and management for information system by selecting the industry having the highest sensitivity for customer's security.

2 Literature Review

In the world, discussion of risk analysis and management process classified two stages, same as figure 1. One stage classified process on risk analysis and management [Mosess, 1992 *etc*]. The other

stage classified process of which risk management included risk analysis [Kim, 1994 *etc*].

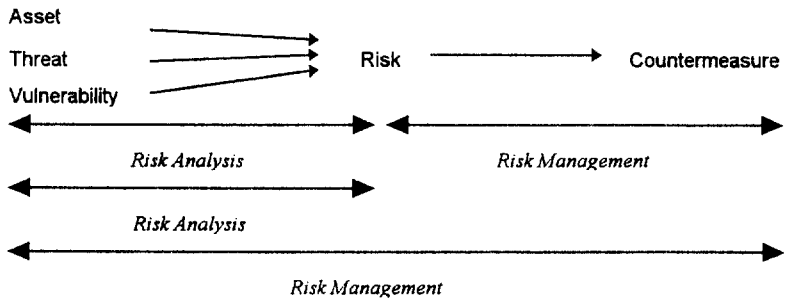

Figure 1. The Process of Risk Analysis and Management

Smith (1993) states that Risk analysis and management are an art not a science, a finger in the wind, and a feel for events. It uses intuition and depends a deep and comprehensive study of not only the enterprise concerned, its culture, its direction, and its history but also a security methodology and more so than computing skill. Namely, it is not just about computing.

Based on Risk analysis and management model of figure 1 or papers, this paper products risk analysis and management process.

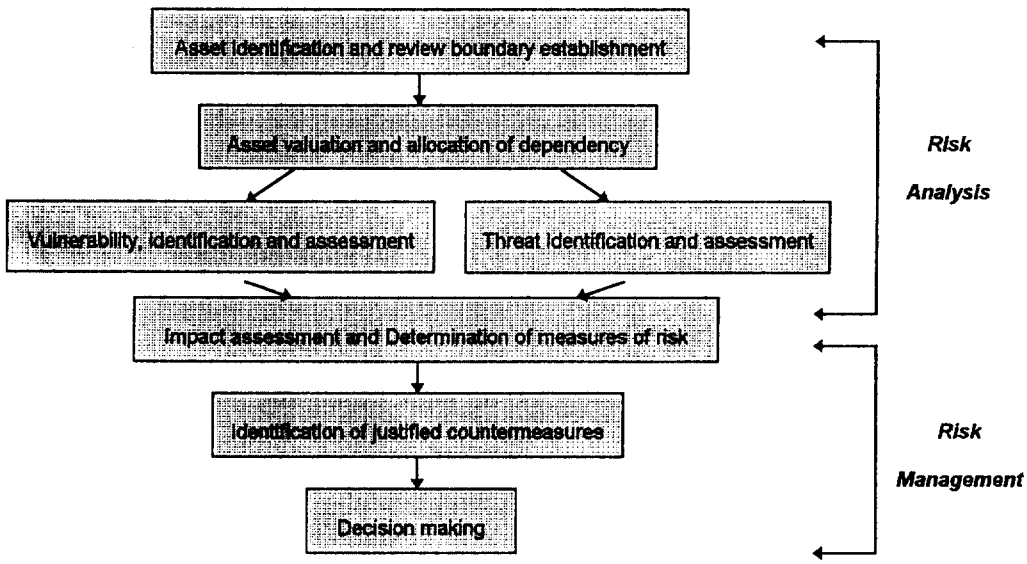

Figure 2. The Process of Risk Analysis and Management
[CRAMM Manual, 1996; Kim, 1994 *etc*]

2.1.1 Asset identification and review boundary establishment

- Asset identification [Glover et al.]

As with the simple model of this thesis, the first component to be identified must be the assets that comprise the system. After all it is the asset that requires the protection. Obviously without assets there is no requirement for security !

- Review boundary establishment [Glover et al.]

Once all of the assets which comprise the system have been identified, the 'boundary' of the review can be established. It is imperative that nothing left outside of the boundary which could impinge on the security of the system.

2.1.2 Asset valuation and allocation of dependency

Asset valuation

In order to decide how much effort should be applied to protect a particular computer, the overall worth of its data must be sensibly assessed [Smith, 1993]. The values of H/W and support facilities during the replacement such as buildings are easily expressed in terms of replacement costs. However the worth of information or data is difficult to determine. For a cost - effective security program, we need to be able to identify the worth of each item of data and concentrate the security resources on those which are the most valuable or critical. Loss of data or loss of the computing facility will result in consequential effects such as loss of market share or damage to reputation or market confidence.

Consequentially, valuation of assets assessed ownership of information and classified information on attributes (confidentiality, integrity, continuity or availability) of information.

Allocation of Dependency [Mosess]

There are relationships between the three asset types. Data assets are dependent on physical assets for input, output, processing and storage, and on software assets. Software assets are dependent on physical assets for storage and processing, and in some cases on other software assets. Some physical assets are dependent on others. Thus a threat manifestation on a physical or software asset could have implications for the assets which are dependent on the physical or software asset.

2.1.3 Threat source identification and assessment

In conformity of various scholars' papers and serious international publicity of organization, the authors of this thesis classify threats same as below *figure 3.*

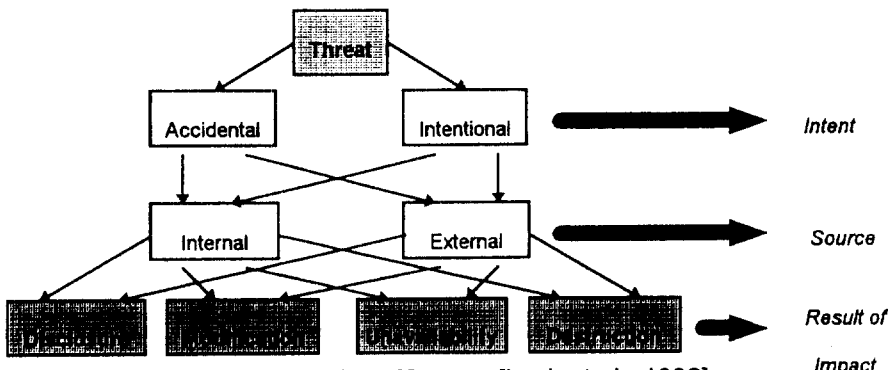

Figure 3. The Classification of Impacts [Loch et al., 1992]

2.1.4 Vulnerability, identification and assessment

Gilbert (1991) states that Vulnerability is defined as the state of system opening to threat. According to Gilbert's definition, vulnerability model is the same as figure 2-3(a). That is, vulnerability is defined the lack of security service (or Countermeasure) like the case of 'A4'. In the case of 'A2', exposure appears on account of the weakness of countermeasure. In the case of 'A1', safeguard is caused by perfectly the security service.

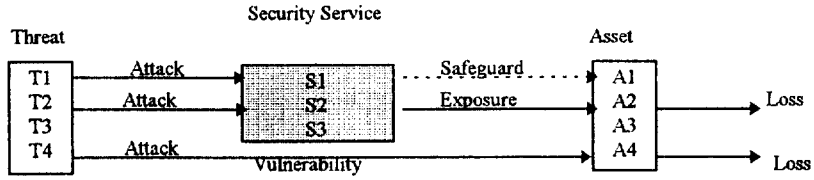

Figure 4. The Model of Vulnerability

2.1.5 Impact assessment and Determination of measures of risk (*See figure 3*)

- From the assessed impacts, one can establish measures of risk of disclosure, modification, unavailability and destruction [Mosess].
- Result of impacts was classified on first and second [Glover *et al.*, 1987].
  - Resultant primary impacts on data could be one or more of disclosure, modification, unavailability and destruction-whilst resultant primary impacts on physical assets could be unavailability or destruction.
  - It is now worth returning to the fact that the manifestation of some threats on physical assets could have implications for the data assets i.e. "secondary impacts". For example, a deliberate threat to a physical asset could have a secondary impact by making the data unavailable. Also, the destruction of a physical asset-say from willful damage by fire-could result in the negation of countermeasures directed at preventing disclosure or modification of data. A similar effect could result from the manifestation of an accidental threat to a physical asset.

2.1.6 Identification of justified countermeasures [Glover *et al.*, 1987]

The method which are the adoptions of countermeasure (or safeguards) are used to manage the identified risk; these are best described-in model terms-grouped to types. 7 types: *Avoidance* (**A**), *Transfer* (**T**), *Reduction of Threat* (**RT**), *Reduction of Vulnerability* (**RV**), *Reduction of Impact* (**RI**), *Detection* (**D**), and *Recovery* (**R**).

2.1.7 Decision making [Mosess]

It was a stage for selection of countermeasures and security services according to criteria of following:

① for a current system, assessment of the need for existing countermeasures and security services

by comparing them with those justified by the determined measures of risks.

② pre-set organizational policy, for example where it has been determined that certain countermeasures and security services will be implemented regardless of the measures of risks.

③ time constraints, for example where only countermeasures and security services which can be implemented before a certain date will be selected.

④ money constraints, for example where only high priority countermeasures and security services can be implemented because of budget constraints.

⑤ technical constraints, for example where some countermeasures and security services cannot be implemented in an existing system because of technical reasons.

⑥ culture constraints, for example where some countermeasures such as certain biometrics devices may not be acceptable because of personnel attitudes.

Smith (1993) states that the analyst can best be likened to the medical practitioner. Ours doctors sometimes call us forward for regular checks, but more often we go to see them when we feel or suspect a problem. The doctor will talk to us, study our history and lifestyle, and apply standard tests before making a diagnosis based on experience and observation. The doctor will recommend a treatment and monitor our progress back to health.

2.2 History Review

Review historical key issues affecting risk analysis over the world.

- Under the auspices of a major European Commission project, a Consortium of European companies led by BIS has successfully produced the strategy for standard risk analysis and management "claims structure". It is based partly on the views and expressed needs of a large number of organizations across Europe and was refined during evaluations of the 12 principle risk analysis methods available in Europe. It encompasses a number of proposed action, including promulgation of the "claims structure" as a preferred approach across Europe and inclusion of the "claims structure" in international standards.
- In 1994, IEC (International Electrotechnical Commission) of ISO (International Organization for Standardization) is processing standardization of risk analysis using " Guidelines for the Management of IT Security ".
- In 1974, FIPS PUB 65 (Federal Information Processing Standards Publications 65) are issued by the National Institute of standards and technology (NIST)-formerly known as the National Bureau of Standard (under the influence of Department of Commerce), and its name was "Guideline for Automatic Data Processing Physical Security and Risk Management". Risk analysis method has ALE (Annual Loss Exposure).
- On August 1, 1979, FIPS PUB 65 (Federal Information Processing Standards Publications 65) are issued by the National Institute of standards and technology (NIST)-formerly known as the

National Bureau of Standard (under the influence of Department of Commerce), and its name was "Guideline for Automatic Data Processing Risk Analysis". Risk analysis method has ALE (Annual Loss Exposure).

- On September 27, 1994, The White house announced that President Clinton had signed Presidential Decision directive 29 (PDD-29). The fact sheet accompanying The White house announcement on PDD-29, stated that Process should be based on sound threat analysis and risk management practices. On November 21, 1994, the U.S. Security Policy Board Staff issued a report entitled "CREATING A NEW ORDER IN U.S. SECURITY POLICY". The report presents the best means of reorganizing current security policy structures to achieve the objectives set forth in PDD-29.

2.3 State of Art

We will require a taxonomy by which we can survey and compare many current security analyses and design methods. Because we will encounter strong indications that security concerns should be incorporated in all system analyses and design methods, this framework must be meaningful to the general information systems audience. A simple taxonomy of methodological "generations" will relate the broader information systems security methods to the perspective of the broader information systems development community. By using the general characteristics of IS analysis and design method, we can compare the evolution of broader IS development methods.

The generation metaphor is useful because it allows a comparison of other dissimilar methods by focusing on their intellectual evolution in response to a changing context. Certain conceptual aspects of the methods (such as assumptions or objectives) can thus be used for classification purposes [Baskerville, 1993].

Generations of Method	Primary Features	System Development Methods and Typical Tools	Security Development Methods and Typical Tools	Seminal Security Works
First-Generation: Checklist Methods (1972-)	Map of limited solutions onto the information problem	Vendor's technical sales procedures & literature	Security checklists & risk analysis	[Krauss, 1972] [Hoyt, 1973] [Courtney, 1977] [Browne, 1979]
Second-Generation: Mechanistic Engineering Methods (1981-)	A partitioned complex solution that matches functional requirements	Top-down engineering, rapid prototyping, system and logic flowcharts	CRAMM, BDSS, control point and exposure analysis matrices, computer questionnaires	[Parker, 1981] [Fisher, 1984]
Third-Generation: Logical Transformation	Highly abstracted design expressing problem and solution space	Structured analysis, data modeling, information engineering, soft	Logical controls design, data flow diagrams	[Baskerville, 1988]

al Methods (1988 --)		system, data flow and entity relationship diagrams		

Table 1. The Classification of Methodologies of Risk Analysis and Management

2.4 Risk analysis methodology

Traditional risk analysis methodology is risk preference(utility)theory, mean variance efficiency criterion, ruin probability, and statistical theory distribution, etc. Specially, risk analysis methodology of IS consists of quantitative and qualitative methodology.

The term *quantitative* usually means risk analysis that calculates threat impact, frequency, and possibility mathematically. Generally, an annualized loss expectancy (ALE) is obtained by multiplying the expected loss per harmful event by the number of times the harmful event is expected to occur in a year's time. The term *Qualitative*, however, indicates a more subjective approach in which threats and assets are given rankings (from 1 to 5, for example) based on the knowledge and judgment of those doing the analysis.

Quantitative risk analysis methodology of IS has formula, probability distribution estimate, stochastic dominance, scoring, and simulation, etc. Qualitative risk analysis methodology of IS has Delphi, scenario, fuzzy metrics, and questionnaires, etc.

Selection of risk analysis methodology considers cost, complexity, validity, and adaptation, etc. Combinatorial risk analysis methodology of IS has value chain analysis [Rainer, Snyder & Carr, 1991] and standard of choice of risk analysis [Perry & Kuong, 1981], etc.

	Qualitative Risk Analysis Methodology	Quantitative Risk Analysis Methodology
Advantages	• The terms are readily understood • Any calculation of risk is inherently quite simple • Can be useful when the monetary value of the asset is irrelevant or for practical reason, unknowable. • Facilitate an expedient assessment in that participants need not spend significant amounts of time determining which of the levels is applicable.	• Allow the user to express cost/value in terms of a commonly accepted independent variable. In other word, money has value independent of the object for which worth (cost/value) is being characterized. • Can be applied to virtually all assets and safeguards • Terms are readily understood ("How much is that car worth?", for example). • Supports mathematical and statistical calculation of risk, including the most advanced statistical modeling techniques. • Budgetary and cost-benefit decisions are supported.
Disadvantages	• The coarse granularity of this matrix makes it difficult to be very specific or subtle. • Budgetary decisions or cost-benefit analyses are virtually unsupported. • Results are truly subjective. No independent metric objectivity can	• Expression of cost/value in monetary terms may not be appropriate • Relating generally developed statistics to a specific site may not always be appropriate. • Calculation increase the effort and time required to execute the

Disadvantages	• be obtained beyond the objectivity of the participants in selecting from among the levels alternatives. The question, "Relative to what?" is not readily answered.	• analysis • Some user/audiences may lack confidence in the "black box effect" that results from using the more sophisticated calculative tools this metric requires.

Table 2. Comparing Qualitative with Quantitative Risk Analysis Methodologies

2.5 Review of S/W with Security Design Methodology

2.5.1 Quantitative Methodology

Quantitative methods are invariably based on a document issued in August 1979 by the US Government's National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards(NBS)) of the Department of commerce, entitled Federal Information Processing Standards Publication Number 65-FIPS was never intended to be a standard, was based on the work of Bob Courtney, then of IBM, and forms the basis for such methods as those which have been used by IBM and a major US Government organization, as well as such as RISKCALC, BDSS, RISKWATCH, and IST/RAMP, etc.

2.5.2 Qualitative methodology

A large extent the development of qualitative methods was stimulated by dissatisfaction with quantitative methods. There was a need to be able to properly identify values of data assets in relation to the potential effects of impacts that were really impossible and illogical to present purely in financial terms, for example endangerment of personal safety, and to assess the level or likelihood of threat source manifestation and level of seriousness of vulnerabilities without subjective specification of frequency of occurrence and other figures. A variety of qualitative methods have been developed over recent years, and there have been extremes of detail and complexity. Some have been very general in nature, for example, a team of people meeting to decide qualitative, such as high/medium/low figures on a group subjective basis; fortunately these approaches, lacking rigor, have almost disappeared from the market-place. Others have involved extremely complex formulae which have only been understandable to the approach designer. Some attempts have been made to use pure expert system based approaches, but thus far the size of the task in hand has proved too difficult and time-consuming. The complexity of those methods and automated support are relatively few in number. S/W of Security design methodology is LAVA, CRAMM, etc.

3. Overview of The CRAMM

CRAMM is a methodology for Information Technology (IT) security developed by the U.K. Government Central Computer and Telecommunications Agency (CCTA), of Her Majesty's Treasury, with assistance from British Information Service (B.I.S.) Applied Systems Limited. The IT Security and

Privacy Group of CCTA is the National Authority for advising British Government Departments on all aspects of the processing unclassified but sensitive (UBS) data.

In 1985 the CCTA initiated a study to examine existing methods for conducting security reviews with the purpose of identifying and recommending a suitable method for use by central government departments processing UBS information. Because none of the methods examined during the study were appropriate, a new method was developed to conform with the requirements specified by CCTA in the initial study.

The method developed is known as the CCTA Risk Analysis and Management Method (CRAMM) and is now available to both public and private organizations.

4 Case Study

4.1 Present Condition of XX Credit Card Co., Ltd.

XX Credit Card Co., Ltd. offers services; factoring, credit card, mail order sales, lease, and insurance agency, and consists of Susomoon, Pusan, Youido, Daegoo, Kwangwhamoon branch, and the main office of Youksam. Information system of XX Credit Card Co., Ltd. is the mainframe system on the head office, and is managed by the information support team in the main office. The information support team is composed of 6 parts; planning, communication, system, developing I, developing II, and information. Also it has 32 personnels. Namely, the information support team is authorized to do security and EDPA (Electronic Data Processing Audit) of the information system of XX Credit Card Co., Ltd.

4.2 Analysis of Asset

4.2.1 Classification of Data Asset

Privacy information with Credit Card service is classified on 15 groups.

The number of group	Contents
1	Card Number
2	Card Number, Password
3	Card Number, Resident Registration Number
4	Card Number, Resident Registration Number, Password
5	Card Number, Resident Registration Number, Password, Name
6	Resident Registration Number, Password
7	Resident Registration Number, Name
8	Resident Registration Number, Password, Name, Settlement Account
9	Name, Work Site (Address, Name, Phone Number, Level)
10	Name, Home(Address, Number)
11	Name, Address(Home, Work Site), Home Phone Number, Money using Card
12	Name, Home (Address, Phone Number), Money using

	Card, Name of Joining Site
13	Name, Name of Work Site, Home Phone Number, Delayed Money
14	Resident Registration Number, Name, Outside Bad Information
15	Name, Resident Registration Number, Content of Guarantee, Content of Lending

Table 3. Classification of Data Assets

The individual data has no meaning. Because of characteristic of credit card business, the individual data has not threat and vulnerability. No impacts. That is, no security need. However if we group data asset, it has meaning. Namely, data asset has threat, vulnerability and impact, and needs security.

4.2.3 Classification of S/W Asset

S/W assets are distributed into 2 parts. One is system S/W. The other is A/P S/W. System S/W is composed of batch tool, IBM O/S, TANDEM O/S, TANDEM TCP/IP S/W. A/P S/W is consisted of client management S/W, sale management S/W, demand and collection management S/W, and delay management S/W. Individual A/P S/W is name grouping sub-A/P S/W.

Name of grouping A/P S/W	Contents
Client Management S/W	● management of client application & receipt ● management of card issue & delivery ● management of transaction suspense of client
Sale Management S/W	● management of permission of using card ● management of actual result of card commodity (general purchase, allotment buy, cash service etc.) ● management of cash payment of joining site according to use card
Demand & Collection Management S/W	● management of demand of using card ● management of collection of using card
Delay Management S/W	● management of general delay ● management of long term delay ● management of starting of law procedure ● management of special bond

Table 4. Classification of S/W Assets

4.2.3 Classification of Physical Assets

According to criteria of CRAMM, physical assets are classified.

Class	Sub-Class	Type	Asset Name
H/W	CPU	Mainframe	IBM Host CPU
		Minicomputer	TANDEM CPU
		Multi-User Micro Computer	ACS Server
			Server
	Storage Device	Disk Drive	TANDEM Storage Disk

		Tape Drive	TANDEM Storage Drive
		Disk Pack-Exchangeable	IBM Host Storage Disk
			TANDEM Storage Disk Pack
		Magnetic Tape	IBM Host Storage Tape
			TANDEM Storage Tape
	I/O Device	Remote Intelligent Terminal	CD
		Remote Dumb Terminal	Banking T
		Local Dumb Terminal	Dummy
		Card Punch	Encoder
		Optical Character Reader	Scanner
		Printer	IBM Host I/O Device
			SSM 7000
			TANDEM I/O Device
			Word Printer
	Network Processor	Intelligent Network Controller	Emulator
			IBM Host Network Processor
			TANDEM Network Processor
	Personal Computer		PC
Communication	LAN Equipment	Ethernet	LAN Card
			TANDEM Communication
	WAN Equipment	MODEM	WAN MODEM
	Internal Communication	Inter-Processor Link	Gateway, Router
		Terminal Link	HUB
Environmental		Air Conditioning	ETC
		Power	ETC 1
		Water	ETC 2

Table 5. Classification of Physical Assets

The distinction of class, sub-class, type is followed by the guideline of CRAMM. The asset name is peculiarly followed after the asset name of XX Credit Card Co., Ltd.

4.3 Assessment of Assets

4.3.1 Assessment of Data Assets

The data asset valuations were established by interviewing the owners of particular data assets, or others who could speak authoritatively about the data. The "data owners" or their representatives were asked to outline the worst scenario which might result from the impacts list.

Data Asset	Unavailability			Destruction	Disclosure		Modification	
	Inconvenient	Serious	Disastrous		Staff	Outsiders	Accidental	Deliberate
1	1	0	0	2	4	3	1	1
2	1	0	0	2	4	3	1	1

3	1	0	0	1	4	3	0	0
4	1	0	0	1	4	3	1	1
5	1	0	0	1	4	3	1	1
6	0	0	0	0	3	2	0	0
7	0	0	0	0	3	3	1	1
8	0	0	0	0	3	3	4	4
9	0	0	0	0	5	5	1	1
10	0	0	0	0	2	1	0	0
11	0	0	0	0	3	2	1	1
12	0	0	0	0	5	3	1	1
13	0	0	0	0	2	3	1	1
14	0	0	0	0	2	2	2	2
15	0	0	0	0	2	1	1	1

Table 6. Assessment of Data Assets

4.3.2 Impacts

Impact		Valuation
Unavailability	Inconvenient (1 day)	
	Serious (3days)	
	Disastrous (5days)	
Destruction (in terms of replacement cost for S/W)		
Disclosure	to Staff	
	to Outsiders	
Modification	Accidental	
	Deliberate	

Table 7. Table for Assessment of Data and S/W Assets

On asset valuation, existing countermeasures were usually ignored to avoid making assumptions about their effectiveness.

Each of the above impacts may affect the user with results in one or more of the following areas:

- User Disruption
- Financial Loss
- Embarrassment
- Personal Safety Implications
- Personal Privacy Implications
- Legal Implications
- Breach of Commercial Confidence

Guidelines are used to assign a numerical value on a scale of 1(Low) to 10(High) to each impact, reflecting the severity of the scenario described. The impact is defined with attributes (confidentiality, integrity, and availability) of information. The relationship between impacts and attributes (confidentiality, integrity, and availability) of information, that is theory and practice following same as:

- Unavailability = *Reverse* of Availability
- Destruction = *Ultimately Reverse* of Availability
- Disclosure = *Reverse* of Confidentiality

- Modification = *Reverse* of Integrity

4.3.3 Assessment of S/W Assets

The S/W asset valuations above were established by interviewing personnel responsible for particular S/W assets, or who could speak authoritatively about them. These "S/W owners" or their representative were asked to outline the worst scenario which might result from the impacts list.

S/W Asset	Unavailability			Disclosure		Modification	
	Inconvenient	Serious	Disaster	to Staff	to Outsiders	Accidental	Deliberate
System	1	4	7	0	0	0	0
A/P	0	0	0	0	0	0	0

Table 8. Assessment of S/W Assets

No each system S/W, which is single processed, means actual working site. Therefore system S/W is evaluated, grouping solo system S/W.

About impacts, all of each A/P S/W(client management, sale management, demand and collection management, and delay management) is evaluated as "0" score. Consequently, all of individual A/P S/W is displayed as name of one A/P S/W.

The destruction, one of impacts, is omitted from list of S/W impacts. Because, in S/W valuation, assessment of the destruction is replaced as financial cost of:

Name of S/W		Value (pound)
System	Batch Tool	81,229
	IBM O/S	981,293
	TANDEM O/S	107,254
	TANDEM TCP/IP	7,100
A/P	Client Management	18,898
	Sale Management	10,150
	Demand & Collection Management	18,878
	Delay Management	29,294

Table 9. Assessment of S/W Assets

4.3.3 Assessment of Physical Assets

Physical assets are valued according to the replacement or reconstruction cost of the individual asset. Namely, asset value = acquisition cost + capital expenditure (no considering revenue expenditure) - depreciation expense.

Class	Sub-Class	Type	Asset Name	Value (Pound)
H/W	CPU	Mainframe	IBM Host CPU	19,700
		Minicomputer	TANDEM CPU	39,627
		Micro Computer	ACS Server	58,485

			Server	40,631
	Storage Device	Disk Drive	TANDEM Storage Disk	8,786
		Tape Drive	TANDEM Storage Drive	3,607
		Disk Pack-Exchangeable	IBM Host Storage Disk	235,424
			TANDEM Storage Disk Pack	9,793
		Magnetic Tape	IBM Host Storage Tape	28,094
			TANDEM Storage Tape	1,512
	I/O Device	Remote Intelligent Terminal	CD	18,806
		Remote Dumb Terminal	Banking T	290,503
		Local Dumb Terminal	Dummy	762
		Card Punch	Encoder	4,114
		Optical Character Reader	Scanner	529
		Printer	IBM Host I/O Device	3,231
			SSM 7000	58,485
			TANDEM I/O Device	9,842
			Word Printer	34,249
	Network Processor	Intelligent Network Controller	Emulator	1,050
			IBM Host Network Processor	76,542
			TANDEM Network Processor	18,288
	Personal Computer		PC	81,108
Commu nication	LAN Equipment	Ethernet	LAN Card	8,441
			TANDEM Communication	1,438
	WAN Equipment	MODEM	WAN MODEM	12,635
	Internal Communication	Inter-Processor Link	Gateway, Router	68,575
		Terminal Link	HUB	20,312
Environ mental		Air Conditioning	ETC	36,639
		Power	ETC 1	8,710
		Water	ETC 2	642

Table 10. Assessment of Physical Assets

4.5 Threat and Vulnerability Assessments

The level of the threat and vulnerabilities to each asset group have been determined by serious objective questionnaires (over 1,000). Each threat and vulnerability to an asset group is given a rating of either high, medium or low according to the total score for the relevant questionnaires. The overall threat and vulnerability assessments for each threat type are shown against each asset group to which the threat applies.

Threat	Type	Asset Group	Assessment
Physical Access	Questionnaire	All of Assets	Medium
Personnel	Questionnaire	All of Assets	Low
Fire(Installation /Room)	Threat	Host Room	Low
	Vulnerability	Host Room	High
Fire(Building)	Threat	K LB Plaza	Low
	Vulnerability	KLB Plaza	Low
Water Damage(Room)	Threat	Host Room	Medium
	Vulnerability	Host Room	High

Natural Disaster	Threat	KLB Plaza	Low
	Vulnerability	KLB Plaza	Medium
Staff Shortage	Threat	All of Data	Low
	Vulnerability	All of Data	Medium
Willful Damage by Outsiders	Threat	KLB Plaza	Low
	Vulnerability	KLB Plaza	High
Willful Damage by Staff	Threat	Host Room	Low
	Vulnerability	Host Room	High
Theft by Outsiders	Threat	KLB Plaza	High
	Vulnerability	KLB Plaza	Low
Theft by Staff	Threat	XX Credit Card Co. Ltd.	Low
	Vulnerability	XX Credit Card Co. Ltd.	Low
System Infiltration by Outsiders	Threat	System	Low
	Vulnerability	System	High
System Infiltration by Staff	Threat	System	Low
	Vulnerability	System	High
Misuse of Resources	Threat	System	Medium
	Vulnerability	System	High
CPU Failure	Threat	IBM Host CPU, TANDEM CPU, Server, ACS Server	High
	Vulnerability	IBM Host CPU, TANDEM CPU, Server, ACS Server	High
Storage Failure	Threat	Disk Drive, Tape Drive, Disk Pack-Exchangeable, Magnetic Tape	High
	Vulnerability	Disk Drive, Tape Drive, Disk Pack - Exchangeable, Magnetic Tape	High
I/O Failure	Threat	Remote Intelligent Terminal, Local Dumb Terminal, Remote Dumb Terminal, Printer, Card Punch, Optical Character Reader,	Medium
	Vulnerability	Remote Intelligent Terminal, Local Dumb Terminal, Remote Dumb Terminal, Printer, Card Punch, Optical Character Reader,	Low
Network Processor Failure	Threat	IBM Host Network Process, TANDEM Network Processor, Emulator	Medium
	Vulnerability	IBM Host Network Process, TANDEM Network Processor, Emulator	Medium
WAN Equipment Failure	Threat	WAN Equipment	Medium
	Vulnerability	WAN Equipment	High
LAN Failure	Threat	LAN Equipment	Medium
	Vulnerability	LAN Equipment	High
Power Failure	Threat	KLB Plaza	Low
	Vulnerability	KLB Plaza	Low
Environmental Failure	Threat	System	Medium
	Vulnerability	System	Low
System Failure	Threat	System	High
	Vulnerability	System	Medium

Operator Error	Threat	IBM Host CPU, TANDEM CPU, Server, ACS Server	Medium
	Vulnerability	IBM Host CPU, TANDEM CPU, Server, ACS Server	Low
WAN Operator Error	Threat	WAN Equipment	Low
	Vulnerability	WAN Equipment	Low
LAN Operator Error	Threat	LAN Equipment	Low
	Vulnerability	LAN Equipment	Low
Application Programmer Error	Threat	All of Data	High
	Vulnerability	All of Data	High
System Programmer Error	Threat	System	Low
	Vulnerability	System	High
Maintenance	Threat	System	Medium
	Vulnerability	System	High
User Error	Threat	All of Data	High
	Vulnerability	All of Data	Low
Stand Alone Microcomputer Failure	Threat	PC	Low
	Vulnerability	PC	High

Table 11. Assessment of Threats and Vulnerabilities

4. Findings

4.6.1 Assessment of Security Need

Once the assets have been valued, and the threat and vulnerabilities assessed, the security needs for system can be established. The security needs are an indication of the risk and thus the level of protection that the system will require against each threat. The security needs are in a range from 1 to 5. 1 indicates a requirement for baseline countermeasures only and 5 the highest security requirement

Consequently, according to combination of rating of the threat (*H*igh, *M*edium, *L*ow) and the vulnerability (*H*igh, *M*edium, *L*ow) and the asset (1, 2, 3, 4, 5, 6, 7, 8, 9, 10), security need is decided.

Name of Threat & Vulnerability	Asset Group	Security Need								
		P	U			D	DI		M	
			1	3	5	9	S	O	A	D
Fire (Installation/Room)	Host Room	5	1	2	4	1	0	0	0	0
Fire (Building)	KLB Plaza	4	1	1	3	1	0	0	0	0
Water Damage (Room)	Host Room	5	1	3	4	1	0	0	0	0
Water Damage (Building)	KLB Plaza	5	1	2	4	1	0	0	0	0
Natural Disaster	KLB Plaza	5	1	2	3	1	0	0	0	0
Staff Shortage	1	0	1	0	0	0	0	0	0	0
	2	0	1	0	0	0	0	0	0	0
	3	0	1	0	0	0	0	0	0	0
	4	0	1	0	0	0	0	0	0	0
	5	0	1	0	0	0	0	0	0	0
	6	0	0	0	0	0	0	0	0	0
	7	0	0	0	0	0	0	0	0	0
	8	0	0	0	0	0	0	0	0	0
	9	0	0	0	0	0	0	0	0	0
	10	0	0	0	0	0	0	0	0	0
	11	0	0	0	0	0	0	0	0	0
	12	0	0	0	0	0	0	0	0	0

	13	0	0	0	0	0	0	0	0	0
	14	0	0	0	0	0	0	0	0	0
	15	0	0	0	0	0	0	0	0	0
Willful Damage by Outsiders	KLB Plaza	5	1	2	4	1	0	0	0	0
Willful Damage by Staff	Host Room	5	1	2	4	1	0	0	0	0
Theft by Outsiders	KLB Plaza	5	1	2	4	1	0	3	0	0
Theft by Staff	XX Co., Ltd.	4	1	1	3	1	2	0	0	0
System Infiltration by Outsiders	System	4	1	2	4	1	0	3	0	2
System Infiltration by Staff	System	4	1	2	4	1	3	0	0	2
Misuse of Resources	System	0	1	3	4	0	0	0	0	0
CPU Failure	IBM Host CPU	0	2	3	5	0	0	0	0	0
	TANDEM CPU	0	2	3	5	0	0	0	0	0
	Server	0	2	3	5	0	0	0	0	0
	ACS Server	0	2	3	5	0	0	0	0	0
Storage Failure	Disk Drive	0	2	3	5	2	0	0	0	0
	Tape Drive	0	2	3	5	2	0	0	0	0
	Disk Pack-Exchangeable	0	2	3	5	2	0	0	0	0
	Magnetic Tape	0	2	3	5	2	0	0	0	0
I/O Failure	Remote Intelligent Terminal	0	1	2	3	0	0	0	0	0
	Local Dumb Terminal	0	1	2	3	5	2	0	0	0
	Remote Dumb Terminal	0	1	2	3	5	2	0	0	0
	Printer	0	1	2	3	5	2	0	0	0
	Card Punch	0	1	2	3	5	2	0	0	0
	Optical Character Reader	0	1	2	3	5	2	0	0	0
Network Processor Failure	IBM Host Network Process	0	1	2	4	0	0	0	0	0
	TANDEM Network Processor	0	1	2	4	0	0	0	0	0
	Emulator	0	1	2	4	0	0	0	0	0
WAN Equipment Failure	WAN Equipment	0	1	3	4	0	0	0	0	0
LAN Equipment Failure	LAN Equipment	0	1	3	4	0	3	0	0	0
Power Failure	KLB Plaza	0	1	1	3	1	0	0	1	0
Environmental Failure	System	0	1	2	3	0	0	0	0	0
System Failure	System	0	1	3	4	1	3	0	3	0
Operator Error	IBM Host CPU	1	1	2	3	1	2	0	2	0
	TANDEM CPU	2	1	2	3	1	2	0	2	0
	Server	2	1	2	3	1	2	0	2	0
	ACS Server	2	1	2	3	1	2	0	2	0
WAN Operator Error	WAN Equipment	1	1	1	3	1	2	2	1	0
LAN Operator Error	LAN Equipment	1	1	1	3	0	2	2	1	0
Application Programmer Error	1	2	2	0	0	2	3	0	2	0
	2	2	2	0	0	2	3	0	2	0
	3	2	2	0	0	2	3	0	0	0
	4	2	2	0	0	2	3	0	2	0

	5	2	2	0	0	2	3	0	2	0
	6	2	0	0	0	0	3	0	0	0
	7	2	0	0	0	0	3	0	2	0
	8	2	0	0	0	0	3	0	3	0
	9	2	0	0	0	0	4	0	2	0
	10	2	0	0	0	0	2	0	0	0
	11	2	0	0	0	0	3	0	2	0
	12	2	0	0	0	0	4	0	2	0
	13	2	0	0	0	0	2	0	2	0
	14	2	0	0	0	0	2	0	2	0
	15	2	0	0	0	0	2	0	2	0
System Programmer Error	System	0	1	2	4	1	3	0	2	0
Maintenance Error	System	4	1	3	4	1	3	3	3	0
User Error	1	0	1	0	0	1	2	2	1	0
	2	0	1	0	0	1	2	2	1	0
	3	0	1	0	0	1	2	2	0	0
	4	0	1	0	0	1	2	2	1	0
	5	0	1	0	0	1	2	2	1	0
	6	0	0	0	0	0	2	1	0	0
	7	0	0	0	0	0	2	2	1	0
	8	0	0	0	0	0	2	2	2	0
	9	0	0	0	0	0	3	3	1	0
	10	0	0	0	0	0	1	1	0	0
	11	0	0	0	0	0	2	1	1	0
	12	0	0	0	0	0	3	2	1	0
	13	0	0	0	0	0	1	1	1	0
	14	0	0	0	0	0	1	1	1	0
	15	0	0	0	0	0	1	1	1	0
Stand Alone Microcomputer Failure	PC	2	1	2	4	1	0	0	0	0

Table 12. Assessment of Security Need

4.6.2 Cost /Benefit Analysis & Countermeasure (appendix A)

Once the security need has been established for each asset group the appropriate countermeasures to protect those asset groups against the relevant impacts must be established.

A countermeasure group consists of a number of countermeasures that deal with the same threats. These countermeasure groups are split into the various security aspects, i.e. those countermeasures which act in the same fashion (procedural, physical, etc.). Each group is further sub-divided into sub-groups.

The countermeasures for each asset group are selected by the following procedure:

- For each threat, there may be several different countermeasure groups, each protecting the assets by a different method.
- For each relevant countermeasure group, all those countermeasures with a security level less than or equal to the security requirement are selected.
- Security Level, applied to countermeasure groups and asset groups, is selected to impacts (unavailability, disclosure, etc.) that have number of security level (1,2,3,4,5), namely no blank. That is, impacts that have not number displaying security level, and do not relate to countermeasure groups and asset groups.

The countermeasures may act in different ways. They may reduce the risk of the threat occurring

(RT), reduce the impact (RI), reduce the vulnerability (RV), detect that a threat has occurred (D), or recover from the occurrence of the threat (R).

The cost means install cost and the level of cost (*H*igh, *M*edium, *L*ow) means difference of install cost by comparison of each countermeasure group in sub-groups of countermeasure (for example, BUILDING FIRE PREVENTION & CONTROL).

The recommended column (*R* of state) indicates the asset level for which the measure has been proposed.

Consequently, The manager would decide to the countermeasure considering type, cost, state, and security level, etc.

5. Developing DSS for Analyzing & Selecting Countermeasures

Because the CRAMM supports many countermeasures, manager difficultly does to analyze them. Therefore, according to support field of decision making, this study develops DSS (Decision Support System), using "Delphi", for analyzing and selecting them. The Delphi is tool developing application program in Window's configuration. It is developed with Borland Co., Ltd.

Look at the model following same as:

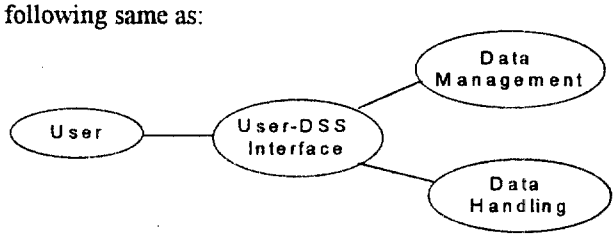

Figure 5. Model of DSS for Analyzing & Selecting Countermeasures

- User-DSS interface : window's configuration, manual data input
- Data management : using engine of Delphi's DB (Database), storage, modification, retrieval
- Data Handling : selection with conditions, graph, and calculating and comparing with averages.

6. Conclusion

6.1 Summary of Contribution

Defining concept through literature review and reviewing process through case study, it explains what is risk analysis and management for information system. When the company installs, countermeasure or security service for information system, it produces criteria. So to speak, when installing security solution for information system, a company is installed to it without plan. Without a scientific plan, a company can not apply security service for information system effectively and efficiently. As this study discloses the weak and strong points of information system, this may be useful for companies to install the information system effectively.

When theoretical risk analysis and management are applied to tool, this research introduces the method overcoming its difference. Consequently, this thesis suggests the idea of problem solving which connects between two fields; theory and practice.

With developing DSS for analyzing and selecting countermeasures, it can be assisted to manager's decision making. Namely, for how well many countermeasures can be arranged?, this thesis produces solutions; DSS model of this study supports ideas for analyzing and selecting countermeasures.

6.2 Limitation & Further Research Issue

The limitations and further research issues are summarizes as follow:

- The CRAMM is only qualitative risk analysis and management method. Hence it for quantitative field is in bias, possible. Consequently, quantitative it solving this bias should parallel qualitative it.
- Database of the CRAMM should update according to flow of time.
- For a question, a number of interviewee need. Because of reducing bias of which an interviewee occurs responding for a question.
- For questions of the CRAMM, sub-question needs for pulling correct response. Because, when responding for question, interviewee doesn't collect data for responding but empirically reply for it. In conclusion, this process is useful for reducing burden of interviewee.
- Developing risk analysis and management tool in fitting Korea.
- Practicing risk analysis and management of several industries for comparing with risk for information system of it.
- Interface part of DSS (Decision support System) is human interface. For improving this part, it is necessary to make relationship between DB (Database) of the CRAMM and DB of DSS for analyzing and selecting countermeasures.

References

1. Commission of the European Communities Security Investigations Projects, Risk Analysis Methods Database, Project S2014-Risk Analysis, Report Number 19744 (S2014/WP08), Version 1.0, Jan. 1993.
2. FIPS PUB 65, Guidelines for Automatic Data Processing Risk Analysis, U.S. Department of Commerce/National Bureau of Standards, Aug. 1979.
3. ISO/IEC JTC1/SC27/WG1 N394, Guidelines for the Management of IT System Security (GMITS): Part3-Risk Analysis Techniques, ISO, 1993.
4. Edwin B. Heinlein, "Principles of Information Systems Security", Computers & Security, Vol. 14, 1995, pp. 197-198.
5. Scott Hill and Martin Smith, "Risk Management & Corporate Security: A Viable Leadership And

Business Solution Designed To Enhance Corporations In The Emerging Marketplace", Computers & Security, Vol. 14, No. 3, 1995, pp. 199-204.

6. Muninder P. Kailay and Peter Jarratt, "RAMeX: a prototype expert system for computer security risk analysis and management", Computers & Security, Vol. 14, No. 5, 1995, pp. 449-463.
7. Paul Caster, "AN ANALYSIS OF TECHNIQUES FOR ASSESSING RISK", THE EDP AUDITOR JOURNAL, VOL. III, 1987, pp. 30-38.
8. Dan Erwin, "The Thirty-Minute Risk Analysis", INFORMATION SYSTEMS SECURITY, FALL, 1994, pp. 37-44.
9. Karen D. Loch, Houston H. Carr, and MerrIII E. Warkentin, "Threats to Information Systems: Today's Reality, Yesterday's Understanding", MIS Quarterly, June 1992, pp. 173-186.
10. Guy L. Copeland and Frederick G. Tompkins, "A New Paradigm for the Development of U.S. Information Security Policy", DATAPRO on Information Security Service, Risk Management, September 1995, pp. 1-20.
11. Frederick G. Tompkins, "How to Select a Risk Analysis Software Package", DATAPRO Classic on Information Security Service, Risk Management, December 1995, pp. 1-5.
12. Frederick G. Tompkins, "Information Security Risk Management", DATAPRO Classic on Information Security Service, Risk Management, December 1995, pp. 1-18.
13. Julie Hollins Freelance, "Information Security in a Service Industry", DATAPRO on Information Security Service, Planning, July 1994, pp. 101-105.
14. Rebecca J. Duncan, Kathleen E. Harvey, and Jackie Hyde, "Computer Security Issues: 1994 Survey", DATAPRO on Information Security Service, Concepts & Issues, January 1995, pp. 201-214.
15. Dr. Paul G. Dorey, "Evaluation and Selection of a Risk Analysis Software Package", Datapro Reports on Information Security, Risk Analysis International, April 1992, pp. 102-108.
16. David L. Drake and Katherine L. Morse, "The Security-Specific Eight-Stage Risk Assessment Methodology", DATAPRO on Information Security Service, Risk Analysis, February 1995, pp. 201-206.
17. Lisa M. Jaworski, "Tandem Threat Scenarios: A Risk Assessment Approach", DATAPRO on Information Security Service, Risk Analysis, February 1994, pp. 101-106.
18. Phillip E. Gardner, "Evaluation of Five Risk Assessment programs", Computer & Security, Vol. 8, No. 6, 1989, pp. 479-485.
19. Will Ozier, "Issues in Quantitative Versus Qualitative Risk Analysis", Datapro Reports on Information Security, Risk Analysis, MARCH 1994, pp. 1-7.
20. _____, "Issues in Quantitative Versus Qualitative Risk Analysis", Datapro Reports on Information Security, Risk Analysis, MARCH 1992, pp. 101-107.
21. Richard Baskerville, "Information Systems Security Design Methods: Implication for Information

System Development", ACM Computing Surveys, Vol. 25, No. 4, December 1993, pp. 375-414.
22. Deborah J. Bodeau, "A Conceptual Model for Computer Security Risk Analysis", IEEE, 1992.
23. R. von Solms and H. van de Haar, S.H. von Solms, and W.J. Caelli, "A framework for information security evaluation", Information & management, Vol. 26, 1994, pp. 143-153.
24. Belden Menkus, "INTRODUCING CRAMM", EDPACS, Vol. XXI, No. 8, February 1994, pp. 1-10.
25. J.H.P. Eloff, L. Labuschagne and K.P. Badenhorst, "A Comparative framework for risk analysis methods", Computer & Security, Vol. 12, No. 6, 1993, pp. 597-603.
26. Bill Farquhar, "One Approach to Risk Assessment", Computer & Security, Vol. 10, No. 1, 1991, pp. 21-23.
27. INSIGHT CONSULTING, "AN OVERVIEW OF CRAMM", 1995.
28. Maureen Harris Cheheyl, Morrie Gasser, George A. Huff, and Jonathan K. Millen, "Verifying Security", Computing Survey, Vol. 13, No. 3, September 1981, pp. 279-339.
29. Allan C. Utter, "THE FOUR ESSENTIALS OF COMPUTER AND INFORMATION SECURITY", INTERNAL AUDITOR, December 1989, pp. 44-50.
30. Carl E. Landwehr, "The Best Available Technologies for Computer Security", COMPUTER, July 1983, pp. 86-100.
31. R. A. Elbra, Computer Security Handbook, NCC Blackwell, 1992.
32. D.W. Roberts, Computer Security, Blenheim Online, 1990.
33. David D. Clark, Computer at Risk, NATIONAL ACADEMY PRESS, 1991.
34. Donn B. Parker, COMPUTER SECURITY MANAGEMENT, A Prentice-Hall Company, 1981.
35. Martin Smith, Commonsense Computer Security, McGRAW-HILL, 1993.
36. Robert K. Yin, CASE STUDY RESEARCH: Design and Methods, SAGE Publications, 1994.
37. _____, APPLICATIONS OF CASE STUDY RESEARCH, SAGE Publications, 1993.
38. Ron Weber, EDP AUDITING: CONCEPTUAL FOUNDATIONS AND PRACTICE, McGRAW-HILL, 1988.
39. Joseph W. Wilkinson, ACCOUNTING INFORMATION SYSTEMS: ESSENTIAL CONCEPTS AND APPLICATIONS, John Wiley & Sons, 1993.
40. 김기윤, 김정덕, "정보시스템 위험분석과 관리", KMIS '94 추계학술대회 논문집, 1994, pp. 277-297.
41. 김기윤, 나관식, 김종석, "보안관리를 위한 위협, 자산, 취약성의 분류체계", 통신정보보호 학회지, 제 5 권, 제 2 호, 1995.
42. 한인구, "전산감사의 의의와 현황", 공인회계사, 논단 2, 1993, pp. 63-68.
43. 김세헌, "금융정보시스템의 안전대책에 관한 연구", 증권학회지, 1990, pp. 41-63.
44. 신장균, "컴퓨터 시스템의 보안평가를 위한 기술적 수준", 통신정보보호 학회지, 제 1 권, 제 2 호, 1991.

45. 김영철, 남길현, "정보시스템 보안과 감사증적 메카니즘", 통신정보보호 학회지, 제 1 권, 제 3 호, 1993.
46. 박영호, 문상재, 김세헌, 강신각, 임주환, "컴퓨터 범죄 방지를 위한 정보통신망의 보호 방안에 관한 연구", 통신정보보호 학회지, 제 4 권, 제 2 호, 1994.
47. 김종기, "정보시스템 보안의 상황적 모형", KMIS '94 추계학술대회 논문집, 1994, pp.299-312.
48. 청산감사법인 시스템감사부, 보안과 위험 관리, 한국광보, 1993.
49. 이형원, 정보시스템 안전대책, 영진 출판사, 1993.
50. 한국전산원, 전산망 보안을 위한 위험 분석 프로그램에 관한 연구, 연구보고서, 1995.
51. 한국전산원, 유닉스 시스템 보안 취약성 분석 및 진단에 관한 연구, 연구보고서, 1995.

Appendix A

< Countermeasures >